Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A method for protecting the contents of an electronic document having a plurality of strings of characters to be encrypted, comprising:

confusing characters belonging to an electronic input document through an invertible scrambler to obtain a confused document, said confused document comprising a plurality of confused characters, and said confusing step comprises adding each string of characters to be encrypted to strings of confused characters obtained by multiplying strings of previously confused characters by respective multiplication constants; and

diffusing said confused document by performing an EXOR operation on it in combination with chaotic characters to obtain an encrypted document.

2. (Previously Presented) The method according to claim 1 wherein said confusing step comprises carrying out operations defined within a Galois field.

3. (Canceled)

4. (Previously Presented) The method of claim 1 wherein, before being multiplied by said multiplication constants, said strings of previously confused characters are delayed.

5. (Previously Presented) The method of claim 1, in which said diffusing step comprises generating chaotic characters through a chaos generator and mixing said strings of confused characters with said chaotic characters.

6. (Original) The method of claim 5 wherein said mixing step comprises performing an exclusive OR operation.

7. (Original) The method of claim 5 wherein said chaos generator implements the function:

$$f_k(x)=Kx(1-x).$$

8. (Original) The method of claim 1, further comprising:

a) loading encryption keys into shift registers of said invertible scrambler and an initial chaotic value into a chaotic-value register;

b) acquiring an input character string;

c) calculating a diffused character string using said input character string, said encryption keys, and the contents of said shift registers;

d) feeding said diffused character string to said shift registers, and issuing a command for a shift operation for said shift registers;

e) repeating b), c) and d) a preset number of times to obtain a plurality of said confused character strings;

f) calculating a subsequent chaotic value, using the contents of said chaotic value register;

g) adding said plurality of confused character strings to said subsequent chaotic value to obtain an encrypted word;

h) storing said subsequent chaotic value in said chaotic value register; and

i) repeating b)-h).

9. (Original) The method of claim 8 wherein c) uses the following relation:

$$s(t) = IN(t) \oplus \sum_{j=0}^{3} c_j \oplus s(t-j)$$

in which *IN(t)* is said input character string, c_j are said encryption keys, *s(t –j)* are the contents of said shift registers, and *s(t)* is said diffused character string.

10. (Original) The method of claim 8 wherein f) uses the following relation:

$$f_k(x)=Kx(1-x);$$

where K is a bifurcation parameter of a chaotic system.

11. (Original) The method of claim 1, comprising decrypting an encrypted document by mixing it with said chaotic characters and unscrambling through an unscrambler opposite to said scrambler.

12. (Previously Presented) The method of claim 3, in which an encrypted document comprises a plurality of encrypted character strings, the method comprising decrypting said encrypted document through a first and a second decryption operation, in cascade, said second decryption operation supplying a plurality of decrypted character strings, said first decryption operation comprising a mixing step wherein said encrypted character strings are mixed with said chaotic characters to obtain a plurality of predecrypted character strings, and said second decryption operation comprising an unscrambling step by subtracting each predecrypted character string from feedback character strings obtained by multiplying said decrypted character strings by said multiplication constants.

13. (Previously Presented) A device for protecting the contents of an electronic document having a plurality of strings of characters to be encrypted, comprising:

a confusion block for confusing an electronic input document, said confusion block comprising an invertible scrambler that supplies a confused document, said confused document comprising a plurality of confused characters, and said confusing step comprises adding each string of characters to be encrypted to strings of confused characters obtained by multiplying said strings of previously confused characters by respective multiplication constants; and

a diffusion block cascade-connected to said confusion block, said diffusion block comprising EXOR mixing means for mixing said confused document with chaotic characters, which supply an encrypted document.

14. (Original) The device of claim 13 wherein said scrambler comprises operators acting within a Galois field.

15. (Original) The device of claim 13 wherein said scrambler comprises an adding element having a first and a second input, said first input receiving a string of characters to be encrypted that belong to said electronic input document; a plurality of shift registers cascade-connected to one another and to said adding element; a plurality of multiplier elements, each having an input connected to an output of a respective shift register and to an own output; a plurality of adding nodes cascade-connected, each adding node having an input connected to said output of a respective multiplier element, an adding node arranged upstream and having a second input connected to a last multiplier element of said multiplier elements, and an adding node arranged downstream and having an output connected to said second input of said adding element.

16. (Original) The device of claim 13 wherein said mixing means comprise an EXOR logic circuit, and said diffusion block comprises a chaos generator.

17. (Original) The device of claim 16 wherein said chaos generator implements the following function:

$$f_K(x)=Kx(1-x);$$

where K is a bifurcation parameter of a chaotic system.

18. (Original) The device of claim 13, comprising, integrated in one first chip, a logic control unit, a scrambler unit connected to said logic control unit, a chaos generator connected to said logic control unit, a secret storage area storing encryption keys for said scrambler unit and an initial chaotic value for said chaos generator.

19. (Original) The device of claim 13, comprising, integrated in a second chip, a logic control unit, an unscrambler unit connected to said logic control unit, a chaos

generator connected to said logic control unit, a secret storage area storing encryption keys for said unscrambler unit and an initial chaotic value for said chaos generator.

20. (Previously Presented) The device of claim 18 wherein said first chip and a second chip each comprise a coating metal layer covering a respective logic control unit, a respective scrambling/unscrambling unit, a respective chaos generator, and a respective secret storage area.

21. (Previously Presented) A method to protect the contents of an electronic document, comprising:

acquiring encryption keys and an initial chaotic value;

acquiring input character strings;

generating confused character strings by calculation using the input character strings, the encryption keys, and previous confused character strings to obtain a confused word;

calculating a current chaotic value from the initial chaotic value; and

calculating an encrypted word by performing an EXOR operation on the confused word and the current chaotic value to obtain an encrypted word.

22. (Previously Presented) The method of claim 21, comprising:

decrypting the encrypted word by adding the encrypted word to a chaotic value identical to the chaotic value and subtracted from a previously decrypted word using an unscrambler element having a structure similar to that of a scrambler that generated the confused word, and further using identical encryption keys.

23. (Previously Presented) A method for protecting the contents of an electronic document, comprising:

loading encryption keys into shift registers of an invertible scrambler and an initial chaotic value into a chaotic-value register;

acquiring an input character string;

calculating a confused character string using the input character string, the encryption keys, and the contents of the shift registers and the following relation:

$$s(t) = IN(t) \oplus \sum_{j=0}^{3} c_j \oplus s(t-j)$$

in which *IN(t)* is said input character string, c_j are said encryption keys, *s(t –j)* are the contents of said shift registers, and *s(t)* is said confused character string; feeding the confused character string to the shift registers and issuing a command for a shift operation for the shift registers;

repeating the acquisition of the input character string, calculating the confused character string, and feeding the confused character string to the shift registers a predetermined number of times to obtain a plurality of confused character strings;

calculating a subsequent chaotic value using the contents of the chaotic value register; and

performing an EXOR operation on the subsequent chaotic value and the plurality of confused character strings to obtain an encrypted word.

24. (Previously Presented) The method for protecting the contents of an electronic document of claim 23, comprising:

decrypting the encrypted word by adding the encrypted word to a chaotic value identical to the chaotic value and subtracted from a previously decrypted word using an unscrambler element having a structure similar to that of a scrambler that generated the confused word, and further using identical encryption keys.

25. (New) A method for protecting the contents of an electronic document having a plurality of strings of characters to be encrypted, comprising:

confusing characters belonging to an electronic input document through an invertible scrambler to obtain a confused document, said confused document comprising a plurality of confused characters, and said confusing step comprises adding each string of

characters to be encrypted to strings of confused characters obtained by multiplying strings of previously confused characters by respective multiplication constants; and

diffusing said confused document by mixing it with chaotic characters to obtain an encrypted document.

26. (New) The method according to claim 25 wherein said confusing step comprises carrying out operations defined within a Galois field.

27. (New) The method of claim 25 wherein, before being multiplied by said multiplication constants, said strings of previously confused characters are delayed.

28. (New) The method of claim 25, in which said diffusing step comprises generating chaotic characters through a chaos generator and mixing said strings of confused characters with said chaotic characters.

29. (New) The method of claim 28 wherein said mixing step comprises performing an EXOR operation.

30. (New) The method of claim 28 wherein said chaos generator implements the function:

$$f_k(x)=Kx(1-x).$$

31. (New) The method of claim 25, further comprising:

a) loading encryption keys into shift registers of said invertible scrambler and an initial chaotic value into a chaotic-value register;

b) acquiring an input character string;

c) calculating a diffused character string using said input character string, said encryption keys, and the contents of said shift registers;

d) feeding said diffused character string to said shift registers, and issuing a command for a shift operation for said shift registers;

e) repeating b), c) and d) a preset number of times to obtain a plurality of said confused character strings;

f) calculating a subsequent chaotic value, using the contents of said chaotic value register;

g) adding said plurality of confused character strings to said subsequent chaotic value to obtain an encrypted word;

h) storing said subsequent chaotic value in said chaotic value register; and

i) repeating b)-h).

32. (New) The method of claim 31 wherein c) uses the following relation:

$$s(t) = IN(t) \oplus \sum_{j=0}^{3} c_j \oplus s(t-j)$$

in which *IN(t)* is said input character string, c_j are said encryption keys, $s(t-j)$ are the contents of said shift registers, and *s(t)* is said diffused character string.

33. (New) The method of claim 31 wherein f) uses the following relation:

$$f_k(x)=Kx(1-x);$$

where K is a bifurcation parameter of a chaotic system.

34. (New) The method of claim 25, comprising decrypting an encrypted document by mixing it with said chaotic characters and unscrambling through an unscrambler opposite to said scrambler.

35. (New) The method of claim 27, in which an encrypted document comprises a plurality of encrypted character strings, the method comprising decrypting said encrypted document through a first and a second decryption operation, in cascade, said second decryption operation supplying a plurality of decrypted character strings, said first decryption

operation comprising a mixing step wherein said encrypted character strings are mixed with said chaotic characters to obtain a plurality of predecrypted character strings, and said second decryption operation comprising an unscrambling step by subtracting each predecrypted character string from feedback character strings obtained by multiplying said decrypted character strings by said multiplication constants.

36. (New) A device for protecting the contents of an electronic document having a plurality of strings of characters to be encrypted, comprising:

a confusion block for confusing an electronic input document, said confusion block comprising an invertible scrambler that supplies a confused document, said confused document comprising a plurality of confused characters, and said confusing block adapted to add each string of characters to be encrypted to strings of confused characters obtained by multiplying strings of previously confused characters by respective multiplication constants; and

a diffusion block cascade-connected to said confusion block, said diffusion block comprising mixing means for mixing said confused document with chaotic characters, which supply an encrypted document.

37. (New) The device of claim 36 wherein said scrambler comprises operators acting within a Galois field.

38. (New) The device of claim 36 wherein said scrambler comprises an adding element having a first and a second input, said first input receiving a string of characters to be encrypted that belong to said electronic input document; a plurality of shift registers cascade-connected to one another and to said adding element; a plurality of multiplier elements, each having an input connected to an output of a respective shift register and to an own output; a plurality of adding nodes cascade-connected, each adding node having an input connected to said output of a respective multiplier element, an adding node arranged upstream and having a second input connected to a last multiplier element of said multiplier elements, and an adding node arranged downstream and having an output connected to said second input of said adding element.

39. (New) The device of claim 36 wherein said mixing means comprise an EXOR logic circuit, and said diffusion block comprises a chaos generator.

40. (New) The device of claim 39 wherein said chaos generator implements the following function:

$$f_K(x)=Kx(1-x);$$

where K is a bifurcation parameter of a chaotic system.

41. (New) The device of claim 36, comprising, integrated in one first chip, a logic control unit, a scrambler unit connected to said logic control unit, a chaos generator connected to said logic control unit, a secret storage area storing encryption keys for said scrambler unit and an initial chaotic value for said chaos generator.

42. (New) The device of claim 36, comprising, integrated in a second chip, a logic control unit, an unscrambler unit connected to said logic control unit, a chaos generator connected to said logic control unit, a secret storage area storing encryption keys for said unscrambler unit and an initial chaotic value for said chaos generator.

43. (New) The device of claim 41 wherein said first chip and a second chip each comprise a coating metal layer covering a respective logic control unit, a respective scrambling/unscrambling unit, a respective chaos generator, and a respective secret storage area.

44. (New) A method to protect the contents of an electronic document, comprising:

acquiring encryption keys and an initial chaotic value;

acquiring input character strings;

generating confused character strings by calculation using the input character strings, the encryption keys, and previously confused character strings to obtain a confused word;

calculating a current chaotic value from the initial chaotic value; and

calculating an encrypted word by performing a mixing operation on the confused word and the current chaotic value to obtain an encrypted word.

45. (New) The method of claim 44, comprising:

decrypting the encrypted word by adding the encrypted word to a chaotic value identical to the chaotic value and subtracted from a previously decrypted word using an unscrambler element having a structure similar to that of a scrambler that generated the confused word, and further using identical encryption keys.

46. (New) A method for protecting the contents of an electronic document, comprising:

loading encryption keys into shift registers of an invertible scrambler and an initial chaotic value into a chaotic-value register;

acquiring an input character string;

calculating a confused character string using the input character string, the encryption keys, and the contents of the shift registers and the following relation:

$$s(t) = IN(t) \oplus \sum_{j=0}^{3} c_j \oplus s(t-j)$$

in which *IN(t)* is said input character string, c_j are said encryption keys, *s(t −j)* are the contents of said shift registers, and *s(t)* is said confused character string; feeding the confused character string to the shift registers and issuing a command for a shift operation for the shift registers;

repeating the acquisition of the input character string, calculating the confused character string, and feeding the confused character string to the shift registers a predetermined number of times to obtain a plurality of confused character strings;

calculating a subsequent chaotic value using the contents of the chaotic value register; and

performing a mixing operation on the subsequent chaotic value and the plurality of confused character strings to obtain an encrypted word.

47. (New) The method for protecting the contents of an electronic document of claim 46, comprising:

decrypting the encrypted word by adding the encrypted word to a chaotic value identical to the chaotic value and subtracted from a previously decrypted word using an unscrambler element having a structure similar to that of a scrambler that generated the confused word, and further using identical encryption keys.